What is claimed is:

1   1.   A method comprising:

2   determining at a first location if a classification

3   parameter is available for Internet Protocol security (IPsec)

4   traffic that indicates a route for the IPsec traffic;

5   if a classification parameter is not available,

6   decrypting the IPsec traffic at a second location if the IPsec

7   traffic is encrypted and determining the classification

8   parameter for the IPsec traffic at the second location; and

9   forwarding the IPsec traffic based on the classification

10   parameter.

1   2.   The method of claim 1 further comprising receiving

2   the IPsec traffic at the first location.

1   3.   The method of claim 1 in which the classification

2   parameter includes a security parameter index (SPI) associated

3   with the IPsec traffic.

1   4.   The method of claim 1 in which the IPsec traffic

2   includes a data packet.

1   5.   The method of claim 1 further comprising forwarding

2   other IPsec traffic included in a traffic stream with the

3   IPsec traffic based on the classification parameter.

1   6.   An article comprising:

2   a machine-readable medium which stores machine-executable

3   instructions, the instructions causing a machine to:

4   determine at a first mechanism if a classification

5   parameter is available for Internet Protocol security (IPsec)

6   traffic that indicates a route for the IPsec traffic;

7   if a classification parameter is not available,

8   decrypt the IPsec traffic at a second mechanism if the IPsec

9   traffic is encrypted and determine the classification

10   parameter for the IPsec traffic at the second mechanism; and

11   forward the IPsec traffic based on the

12   classification parameter.

1   7.   The article of claim 6 further causing a machine to

2   receive the IPsec traffic at the first mechanism.

1   8.   The article of claim 6 in which the classification

2   parameter includes a security parameter index (SPI) associated

3   with the IPsec traffic.

1   9.   The article of claim 6 in which the IPsec traffic

2   includes a data packet.

1   10.   The article of claim 6 further causing a machine to

2   forward other IPsec traffic included in a traffic stream with

3   the IPsec traffic based on the classification parameter.

1   11. A system comprising:

2   a first mechanism configured to communicate with a

3   network, to determine if a classification parameter that

4   indicates a route for a traffic stream is available for a

5   packet included in the traffic stream; and

6   a second mechanism configured to receive the packet from

7   the first mechanism, to perform an encryption procedure on the

8   packet if the packet is encrypted and associated with a known

9   encryption-related key, and, if the classification parameter

10   is available, to forward the packet based on the route for the

11   traffic stream.

1   12. The system of claim 11 further comprising a third

2   mechanism configured to communicate with the first mechanism

3   and with the second mechanism and to determine a

4   classification parameter for the packet if a classification

5   parameter is not available.

1   13. The system of claim 12 in which the second mechanism

2   is also configured to forward the packet to the third

3   mechanism if the packet is not associated with a known

4   encryption-related key.

1   14. The system of claim 12 in which the third mechanism

2   is also configured to, after determining the classification

- 20 -

3   parameter for the packet, forward the classification parameter

4   to the first mechanism.

1   15.   The system of claim 12 in which the third mechanism

2   is also configured to, after determining the

3   encryption-related key for the packet, forward the

4   encryption-related key to the second mechanism so that the

5   second mechanism can perform the encryption-related procedure.

1   16.   The system of claim 12 in which the second mechanism

2   and the third mechanism are both included as part of a fourth

3   mechanism.

1   17.   The system of claim 11 further comprising a

2   plurality of additional mechanisms, each additional mechanism

3   configured to communicate with the first mechanism, to perform

4   an encryption procedure on the packet if the packet is

5   encrypted and associated with a known encryption-related key,

6   and, if the classification parameter is available, to forward

7   the packet based on the route for the traffic stream.

1   18.   The system of claim 11 in which the packet includes

2   an Internet Protocol security data packet.

1   19.   The system of claim 11 in which the traffic stream

2   includes a plurality of Internet Protocol security data

3   packets.

- 21 -

1   20.   The system of claim 11 in which the first mechanism

2   is also configured to forward the packet to the second

3   mechanism if the packet is encrypted.

1   21.   The system of claim 11 in which the route for the

2   traffic stream includes a route through a network.

1   22.   The system of claim 21 in which the network includes

2   an Internet.

1   23.   The system of claim 11 in which the encryption

2   procedure includes encrypting the packet.

1   24.   The system of claim 11 in which the encryption

2   procedure includes decrypting the packet.

1   25.   The system of claim 11 further comprising another

2   mechanism configured to receive the packet from the second

3   mechanism and to forward the packet based on the route to an

4   ultimate destination of the packet.

1   26.   The system of claim 11 in which the first mechanism

2   is also configured to route packets included in the traffic

3   stream based on a load balancing scheme.